



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/688,456	10/16/2000	Craig L. Ogg	39778/RRT/S850	1637
23363	7590	07/25/2008		
CHRISTIE, PARKER & HALE, LLP			EXAMINER	
PO BOX 7068			ELISCA, PIERRE E	
PASADENA, CA 91109-7068				
			ART UNIT	PAPER NUMBER
			3621	
			MAIL DATE	DELIVERY MODE
			07/25/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

---

*Ex parte* CRAIG L. OGG and WILLIAM W. CHOW

---

Appeal 2008-1041  
Application 09/688,456  
Technology Center 3600

---

Decided: July 25, 2008

---

Before HUBERT C. LORIN, JOSEPH A. FISCHETTI, and BIBHU R.  
MOHANTY, *Administrative Patent Judges*.

MOHANTY, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

The Appellants seek our review under 35 U.S.C. § 134 of the final rejection of claims 1-71. We have jurisdiction under 35 U.S.C. § 6(b) (2002). We REVERSE.

## THE INVENTION

The Appellants' claimed invention relates to the secure printing of value bearing items (VBI) which are preferably postage. The system includes one or more cryptographic modules and a central database. The cryptographic modules serve the function of Postal Security Devices (PSD's) and can prevent unauthorized modification of the value bearing items (Specification, 1-3). Claim 1, reproduced below, is representative of the subject matter of appeal.

1. A cryptographic system for securing data on a computer network comprising:
  - a plurality of users coupled to the computer network; and
  - a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users, and each of the plurality of cryptographic devices comprising:
    - a processor programmed to authenticate the plurality of remote users on the computer network for secure processing of a value bearing item (VBI);
    - a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users;
    - a cryptographic engine for cryptographically protecting data;
    - an interface for communicating with the computer network, and
    - a module for processing value for the value bearing item, wherein each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users, wherein each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users, and

wherein each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users.

## THE REJECTIONS

The Examiner relies upon the following as evidence in support of the rejections:

Lewis et al.

US 6,233,565 B1

May 15, 2001

The following rejections are before us for review:

1. Claims 1-71 are rejected under 35 U.S.C. § 102(e) as anticipated by Lewis.

## FINDINGS OF FACT

We find the following enumerated findings of fact are supported at least by a preponderance of the evidence<sup>1</sup>:

1. Lewis does not disclose that each of the plurality of cryptographic devices is remote from the plurality of users (Col. 21:64-67).
2. Lewis does not specifically disclose that each cryptographic device includes a module for processing the value bearing item.
3. Lewis does not specifically disclose that each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users.

---

<sup>1</sup> See *Ethicon, Inc. v. Quigg*, 849 F.2d 1422, 1427 (Fed. Cir. 1988) (explaining the general evidentiary standard for proceedings before the Patent Office).

4. Lewis does not specifically disclose that each of the plurality of cryptographic devices is capable of processing a VBI printing request from any of the plurality of remote users.
5. Lewis does not specifically disclose that each of the plurality of cryptographic devices is capable of generating indicia data for transmitting to any of the plurality of remote users.

## PRINCIPLES OF LAW

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, (Fed. Cir. 1987). Analysis of whether a claim is patentable over the prior art under 35 U.S.C. § 102 begins with a determination of the scope of the claim. We determine the scope of the claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction in light of the Specification as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). The properly interpreted claim must then be compared with the prior art.

## ANALYSIS

The Appellants argue that the rejection of claim 1 is improper because Lewis does not disclose the limitation for “a plurality of cryptographic devices, each of the plurality of cryptographic devices remote from the plurality of users” (Br. 4). The Examiner takes the position that because a

plurality of clients may exist (Ans. 5) that the claim limitation is met by Lewis.

We agree with the Appellants in this regard. Lewis fails to disclose that each of the cryptographic devices is remote from the plurality of users (FF 1). Lewis fails to disclose that the each cryptographic module is remote from the user (Col. 21:64-67).

The Appellants further argue that Lewis does not disclose that each cryptographic device includes a “module for processing the value bearing item” (Br. 5). The Examiner argues that because the purchase server needs not go through the authorization server that this limitation is found in Lewis (Ans. 5).

We agree with the Appellants in this regard. Lewis does not specifically disclose that each cryptographic device includes a module for processing the value bearing item (FF 2). The operation of the purchase server and authorization server cited by the Examiner disclose nothing specifically as to the operation of the cryptographic device.

The Appellants further argue that Lewis does not disclose that “each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users” (Br. 5). The Examiner argues that the cryptographic module 12 of Lewis performs this function (Ans. 6).

We agree with the Appellants in this regard. Lewis does not disclose that each of the plurality of cryptographic devices is capable of authenticating any of the plurality of remote users (FF 3). The Examiner has failed to specifically show where the cryptographic device performs such a function in the Lewis reference.

The Appellants also argue that Lewis fails to disclose that “each of the plurality of cryptographic devices is capable of processing a VBI printing

request” or “capable of generating indicia data” from or to “any of the plurality of remote users” respectively (Br. 6). We agree with the Appellants in both these regards as the Lewis reference does not show the cryptographic devices to perform these functions (FF 4 and 5). We note that the Examiner has failed to respond to these two arguments made by the Appellants in the Answer.

For the reasons above we will not sustain the rejection of claim 1 as anticipated under 35 U.S.C. § 102(e) as being anticipated by Lewis. As the rejection of claims 2-40 fails to cure the deficiency of the rejection, we will also not sustain the rejection of these claims as well.

With regards to claim 41, the Appellants argue that it contains elements similar to those of claim 1 and that the rejection of claim 41 should be reversed for the same reasons as claim 1 (Br. 8). Claim 1 contains a limitation for “authenticating any one of the plurality of remote users by any one of the plurality of cryptographic devices” which we agree is not shown in the Lewis reference (see FF 3). Claim 1 also contains a limitation for “processing value for the value bearing item by any one of the plurality of cryptographic devices” which we also agree is not shown by Lewis (see FF 4).

For the reasons above we will not sustain the rejection of claim 41 as anticipated under 35 U.S.C. § 102(e) as being anticipated by Lewis. As the rejection of claims 42-70 fails to cure the deficiency of the rejection, we will also not sustain the rejection of these claims as well.

CONCLUSIONS OF LAW

We conclude that Appellants have shown that the Examiner erred in rejecting claims 1-71 under 35 U.S.C. § 102(e) as being anticipated by Lewis et al.

DECISION

The Examiner's rejection of claims 1-71 is not sustained.

REVERSED

LV:

CHRISTIE, PARKER & HALE, LLP  
PO BOX 7068  
PASADENA, CA 91109-7068